UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN MATTER OF THE SEARCH OF THE PREMISES LOCATED AT STORAGE UNIT # 1000 ON THE GROUND FLOOR OF AMERICAN SELF STORAGE, 330 TOMPKINS AVENUE, STATEN ISLAND, NY	**TO BE FILED UNDER SEAL** Mag. No. _____ **AFFIDAVIT**

STATE OF NEW YORK)
) ss.
COUNTY OF KINGS)

I, Semyon Ginzburg, being first duly sworn, hereby depose and state as follows:

1. I am a Special Agent of Department of Homeland Security, Homeland Security Investigations ("HSI"), and have been so employed since approximately 2009. I have been trained in various aspects of law enforcement, particularly the investigation of financial fraud cases. During my career, I have participated in and conducted many criminal investigations involving violations of the laws of the United States, including the laws relating to conspiracy, mail fraud, wire fraud, fraud against financial institutions and money laundering. I also have participated in the execution of numerous search warrants and have examined the personal and business records of numerous individuals and companies. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, and various other criminal laws and procedures.

2. This Affidavit is submitted in support of an application for a search warrant authorizing the search and seizure of the premises located at Storage Unit # 1000 on the Ground Floor of American Self Storage, 330 Tompkins Avenue, Staten Island, NY (the

"SUBJECT PREMISES"), for the items specified in Attachment B, which items constitute the evidence of violations of the interstate transportation of stolen property, wire fraud, bank fraud, money laundering, as well as conspiracy to do the same and attempts to do the same, in violation of Title 18, United States Code, Sections 371, 1343, 1349, 1956(h), 1957, 2314, and 2 (collectively, the "SPECIFIED FEDERAL OFFENSES"). I am requesting authority to search all of the SUBJECT PREMISES where the items specified in Attachment B may be found and to photograph, photocopy, or otherwise copy the items listed in Attachment B as instrumentalities, fruits and evidence of crime.

3. I have personally participated in the investigation of the offenses described herein, and am familiar with the facts and circumstances of this investigation from my personal participation. The information contained in this affidavit is based upon my personal observations, conversations with various law enforcement agents, and others, as well as my personal observations and knowledge. All dates set forth below are approximate. All statements are provided in sum and substance and in part. Where specific recorded conversations are described, they are set forth in substance and in part. Because this affidavit is intended to show only that there is sufficient probable cause for the requested warrant, it does not set forth all aspects of the investigation that I or other agents are aware.

BACKGROUND

4. A "booster" is a person who steals goods and merchandise, including, but not limited to, over-the-counter medication (OTC) from retail stores, and other non-prescription health and beauty aid ("HBA") products that can be readily sold in a secondary market.

OTC includes, but is not limited to, Prilosec, Zantac, Claritin, and Mucinex. A "booster" often re-sells the stolen merchandise to a "fence" at a fraction of the retail value.

5. A "fence" is a person who receives stolen goods and merchandise from "boosters" and others in order to re-sell the goods to third parties for profit.

6. SALIM ABUTAIR, a/k/a "Sami," is a resident of Staten Island, New York, who operates as a fence in the New York and New Jersey area. ABUTAIR receives stolen merchandise, including OTC products from boosters, and re-sells those products at a profit to higher-level fences. ABUTAIR operates the following businesses, among others: 833 National Inc.; 75 National Inc.; 88 National Inc.; and 75 National Ink, Inc. (collectively, the "ABUTAIR Entities").

7. MOHAMMED ABUTEER is a resident of Staten Island, New York, who works as a "fence," and is ABUTAIR's partner. In addition, defendant ABUTEER operated MST Sales, Inc., and is the primary or sole signatory on the MST Sales, Inc. bank account.

8. ABUTAIR and ABUTEER conduct their business from the SUBJECT PREMISES.

9. FELIPE PERALTA works with "booster" crews in New Jersey, among other places.

10. On or about November 10, 2010, a Confidential Informant ("CI") was arrested at Fort Dix, Military Base, NJ, for shoplifting at the Fort Dix Commissary. During a post-arrest interview, the CI provided information concerning an organized retail crime ring

which targeted military bases and retail chain stores, such as Target, Wal-Mart and CVS, throughout the country.[1]

11. According to the CI, PERALTA coordinated and directed the CI and other boosters to steal OTC and HBA products, as well as other merchandise. According to the CI, PERALTA directed the CI and other boosters to steal specific products and paid them for the stolen merchandise based on previously set prices. As an example, PERALTA paid boosters $11 for a package of 30-count Crest White Strips, which retailed for approximately $50. The CI and other boosters would then bring the stolen merchandise to PERALTA at an agreed-upon location, where they would receive payment in cash.

12. Subsequent investigation has revealed that ABUTAIR and ABUTEER are part of a large-scale, organized retail theft ring. The ring is comprised of three tiers:

a. "Tier One" is comprised of PERALTA and others who manage the boosters and purchase stolen products from them.

b. Tier One players sell the stolen products to "Second Tier" fences – in this case, ABUTAIR and ABUTEER – who store the stolen products and remove any markings or tags reflecting the retail stores from where they were stolen.

c. The Second Tier fences, in turn, sell stolen products to "Third Tier" distributors, who sell the stolen products at below retail prices to retailers for resale, or directly to consumers.

---

[1] The CI has provided information in this investigation that has proven to be reliable and has been corroborated by independent evidence, including consensually monitored recordings between the CI and individuals engaged in the criminal conduct described herein as well as by the Cooperating Witness. The CI, however, was recently arrested on July 2, 2012 in Glen Allen, Virginia on Grand Larceny and Possession of Burglary Tools charges. The CI remains in custody in Henrico County Jail in Barhamsville, Virginia, and has not been debriefed by law enforcement since his arrest.

13. An analysis of bank records from in or about January 2008 to the present has revealed approximately $634,207 in checks written from the ABUTAIR Entities to PERALTA and/or PERALTA's business. In addition, bank records from in or about January 2008 through the present reveal that the ABUTAIR Entities and MST Sales received wire transfers and checks in excess of $6 million from known Third Tier distributors.

PROBABLE CAUSE

a. Between in or about February 2012 and in or about May 2013, I along with other law enforcement officers conducted surveillance of ABUTAIR and ABUTEER. Among other things, the surveillance revealed that ABUTAIR and ABUTEER resided together in Staten Island, New York, and worked out of a unit adjacent (the "Adjacent Unit") to the SUBJECT PREMISES. During that same period, I along with other law enforcement officers observed ABUTAIR and ABUTEER remove boxes from the Adjacent Unit and load them into delivery vans, and deliver the products to known Third Tier distributors.

14. As of May 19, 2012, the Adjacent Unit had been leased to "Freddy Zoya," which appears to be a variation of the name of one of ABUTAIR's coconspirators. Prior to that time, it was leased to ABUTAIR. A search of law enforcement databases did not reveal any information regarding Freddy Zoya, or the address provided for him, suggesting that both are fictitious.

15. On or about May 24, 2012, investigators visited American Self Storage to interview the property manager (the "Property Manager") regarding ABUTAIR and his activities. The Property Manager informed the investigators that ABUTAIR had recently abandoned a unit in favor of the Adjacent Unit. The property manager showed the

investigators the abandoned unit, where they recovered a handwritten list of HBA products, including quantities. Based on my experience, I know the list to be a list of products targeted by individuals involved in ORC.

16. After recovering the discarded list, I observed the Adjacent Unit from the surrounding hallway. At eye level, I observed a number of holes in the corrugated metal walls, as well as gaps in the corrugated metal walls. From those holes and gaps, I was able to clearly observe piles of products such as Allegra, Rogaine, and Similac stacked throughout the unit. I was informed by the Property Manager that the occupants of the Adjacent Unit, including ABUTAIR, routinely move such products in and out of the Adjacent Unit, and have even offered such products to him and others.

17. In addition to the products that I observed, I also observed what I know to be a "cleaning station" – an area within the unit comprised of a table, on top of which I observed, among other things, lighter fluid bottles and heating guns. Cleaning stations are used by individuals involved in ORC to remove security labels and other identifying labels that could show the true origins of products, such as stickers bearing Target or Walmart logos. Based on my experience, I know that cleaning stations are typically comprised of heating guns, fans, and lighter fluid, which are used to remove the above-described stickers. In addition, the heating guns are used to repackage materials.

18. On or about August 16, 2012, I obtained a search warrant from United States Magistrate Judge Steven M. Gold in the Eastern District of New York to conduct a "sneak and peek" search of the Adjacent Unit.

19. On or about August 21, 2012, I along with other law enforcement officers conducted the court-authorized "sneak and peek" search of the Adjacent Unit, which revealed, among other things, the following:

a. Piles of products such as Allegra, Rogaine, and Similac stacked throughout the unit;

b. Invoices reflecting sales of OTC products by defendants ABUTAIR and ABUTEER to known Third Tier distributors;

c. A "cleaning station"[2] – an area within the SUBJECT PREMISES comprised of a table, on top of which I observed, among other things, lighter fluid bottles and heat guns; and

d. Numerous discarded security labels removed from OTC products.

20. In or about November 2012, I along with other agents approached PERALTA, who agreed to cooperate in this investigation. Among other things, he corroborated information provided by the CI, and informed me that he sold stolen HBA and OTC products to ABUTAIR and ABUTEER.

21. Thereafter, on or about December 14, 2012, I along with other law enforcement officers directed PERALTA to call ABUTAIR and inform ABUTAIR that PERALTA had products available for sale. Thereafter, PERALTA arranged to meet ABUTAIR in the vicinity of Hastings Street in Staten Island, New York. Prior to the meeting, I along with other law enforcement officers provided PERALTA with OTC

[2] Cleaning stations are used by individuals involved in ORC to remove security labels and other identifying labels that could show the true origins of products, such as stickers bearing Target or Walgreens logos. In addition, the heat guns are used to repackage materials

products with an approximate retail value of $5,465. These products included Rogaine, Crest White Strips, Prilosec, Pepcid, Zantac, Abreva and Claritin (collectively the "Stolen Products"). Each package had Rite Aid, CVS, and Walgreens security labels on them. Also, prior to the meeting, I provided PERALTA with a recording device.

22. On or about December 14, 2012, at approximately 2:25 p.m., ABUTEER arrived in the vicinity of Hastings Street in Staten Island, New York, and met with PERALTA. During the meeting, which was consensually recorded, ABUTEER informed PERALTA that ABUTAIR could not make it to the meeting, and helped PERALTA transfer the Stolen Products from the PERALTA's vehicle into ABUTEER's vehicle. Next, PERALTA informed ABUTEER, in sum and substance, that PERALTA and his booster crew were paying off security guards to look the other way to facilitate their theft of OTC products from the stores, and that he would have access to additional products in the future. ABUTEER expressed interest in continuing to work with the PERALTA in the future. Thereafter, ABUTEER presented PERALTA with a check in the amount of $2,352 – the "street value" of the Stolen Products. The check was drawn on an account in the name of one of the ABUTAIR Entities and payable to PERALTA.

23. In or about January 2013, the Property Manager informed law enforcement agents that ABUTAIR and ABUTEER had moved their operations from the Adjacent Unit to the SUBJECT PREMISES.

24. On or about May 22, 2013, law enforcement agents interviewed an employee who works for ABUTAIR and ABUTEER at the SUBJECT PREMISES. At the time law enforcement agents approached the employee, he had just arrived to work at the SUBJECT PREMISES and had opened the door to it. According to the employee, he was hired by

ABUTAIR and ABUTEER approximately one and a half months ago, and he works inside the SUBJECT PREMISES, where he is tasked with among other things removing store security labels from OTC and HBA products. The employee informed law enforcement agents that security tags he removed were from stores such as CVS, Walgreens and Rite-Aid. The employee also stated that another employee used a laptop computer in the SUBJECT PREMISES to generate invoices for ABUTAIR and ABUTEER's customers. Finally, the employee stated that about a week ago ABUTEER gave him a key to the SUBJECT PREMISES, and told the employee to run things with ABUTEER's father because ABUTEER was leaving for Jordan.

25. In addition to information provided by the employee, law enforcement agents were able to observe OTC and HBA products in the SUBJECT PREMISES from the hallway, and are presently securing the SUBJECT PREMISES.

26. Based on the information above and my training and experience, I believe that SUBJECT PREMISES will contain evidence, fruits, and instrumentalities of the Specified Federal Offenses, including but not limited to:

a. HBA products, baby formula packages, OTC medications, and other retail items;

b. documents that establish or show ownership of the SUBJECT PREMISES;

c. ledgers, spreadsheets, receipts, or other business records;

d. lists of customers or suppliers;

e. product or price lists;

f. shipping labels or receipts;

g. address books or contact lists; and,

h. computer equipment used in furtherance of the Specified Federal Offenses.

SEARCH AND SEIZURE OF COMPUTER SYSTEMS

27. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

28. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

29. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

a. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

b. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during

the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 gigabytes (GB) of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 250 million pages of data, which, if printed out, would result in a stack of paper over ten miles high. Further, a 500 GB drive could contain as many as approximately 250 full-run movies or 450,000 songs.

c. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

30. In light of these concerns, I hereby request the Court's permission to search, copy, image and seize the computer hardware (and associated peripherals) that are believed

to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the image or hardware for the evidence described.

DEFINITIONS APPLICABLE TO SEARCH AND SEIZURE OF COMPUTERS

31. The terms records, notes, documents, communications, correspondence, information, programs, applications and materials include all of the items described above in whatever form and by whatever means they may have been created and/or stored. This includes handmade, photographic, mechanical, electrical, electronic (including e-mail, computer files, Internet histories, bookmarks and all other electronic items that may be found on computer hardware in any form), and/or magnetic forms. It also includes items in the form of computer hardware, computer software, computer documentation, passwords, and/or data security devices.

a. Computer hardware consists of all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. This includes any data-processing devices (such as central processing units, memory typewriters, and self-contained “laptop” or “notebook” computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, transistor-like binary devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communication devices (such as routers, modems, cables, and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating

devices); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

b. Computer software is digital information which can be interpreted by a computer and any of its related components to direct the way it works. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (like word-processing, graphics, or spreadsheet programs, utilities, compilers, interpreters, and communications programs).

c. Computer-related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.

d. Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

CONCLUSION

32. Based on the above information, there is probable cause to believe that the Specified Federal Offenses have been committed and that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; or property designed for use, intended for use, or used in committing a crime, as described in Attachment B, are located at the SUBJECT PREMISES. This Affiant requests authority to seize and search such material.

33. Based upon the foregoing, this Affiant respectfully requests that this Court issue a search or the SUBJECT PREMISES, more particularly described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

34. It is further respectfully requested that this Court seal, until further order of this Court, all papers submitted in support of this application, including the Application, Affidavit, and Search Warrant, and the requisite inventory notice (with the exception of one copy of the warrant and the inventory notice that will be left at the SUBJECT PREMISES). Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation and premature disclosure of the contents of this Affidavit and related documents may have a negative impact on this continuing investigation and may jeopardize its effectiveness.

_____
Semyon Ginzburg, Special Agent
Department of Homeland Security,
Homeland Security Investigations

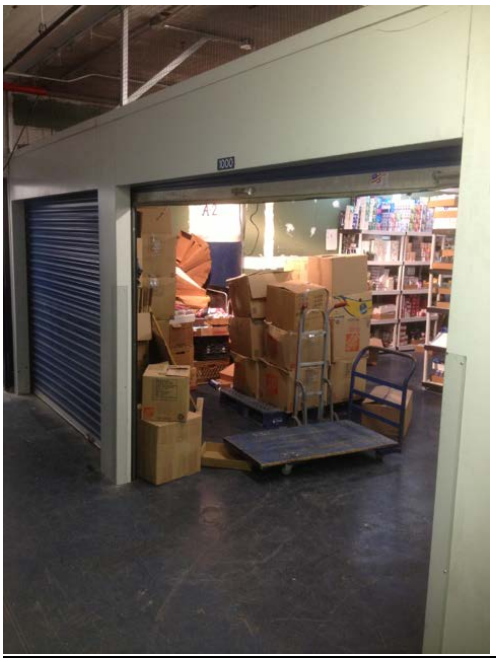
Sworn to before me on the
22nd day of May, 2013

S/ James Orenstein

_____
Honorable James Orenstein
United States Magistrate Judge

ATTACHMENT A

The premises to be searched ("SUBJECT PREMISES") is Storage Unit # 1000 on the Ground Floor of American Self Storage, 330 Tompkins Avenue, Staten Island, NY. The number "1000" appears above the door to the SUBJECT PREMISES, and it is one of two units in that area of the warehouse – the other unit in the area is easily distinguishable and is prominently labeled "1001." The SUBJECT PREMISES is approximately thirty-five feet by forty-five feet. In addition to the door marked "1000" in the front of the unit, there is a pad-locked roll away door on each side of the door marked "1000." One side of the unit is comprised of a ten foot corrugated steel wall, and the other side wall is comprised of sheet rock. The back wall of the unit is a ten foot high solid wall. There is approximately a two foot gap between the walls of the unit and the ceiling on all four sides. Pictures of the SUBJECT PREMISES are included below:



ATTACHMENT B

The SUBJECT PREMISES shall be searched for evidence, fruits, and instrumentalities relating to violations of Title 18, United States Code, Sections 371, 1343, 1349, 1956(h), 1957, 2314, and 2 (the "Specified Federal Offenses"), namely:

1. All health and beauty aid products, baby formula packages, over-the-counter medications, and other retail items;

2. documents that establish or show ownership of the SUBJECT PREMISES;

3. ledgers, spreadsheets, receipts, or other business records;

4. lists of customers or suppliers;

5. product or price lists;

6. shipping labels or receipts;

7. address books or contact lists; and,

8. any documents or things related to the SPECIFIED FEDERAL OFFENSES.

9. As used above, the terms documents, includes documents created, modified or stored in any form, including electronic media such as, but not limited to, desktop computers, laptop computers, iPads, iPhones, Blackberrys, USB storage devices, memory sticks, compact discs, audio tapes, microcassette tapes, audio recording devices with or without internal storage, and video recording devices with or without internal storage.

10. In order to search for the items described above that may be maintained in electronic media, law enforcement personnel seek authorization to search, copy, image and seize the following items for off-site review:

a. any computer equipment and storage device capable of being used to commit, further or store evidence of the offense listed above;

b. any computer equipment used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners;

c. any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC

cards, memory calculators, electronic dialers, electronic notebooks, smartphones and personal digital assistants;

d. any documentation, operating logs and reference manuals regarding the operation of the computer equipment, storage devices or software;

e. any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices or data to be searched;

f. any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data;

g. any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data; and

h. files, records, programs, logs, electronic communications, scanning programs, financial records and routing configuration software.